



19 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

12 Offenlegungsschrift
10 DE 101 43 556 A 1

51 Int. Cl.⁷:
B 60 R 16/02
G 08 C 17/02

21 Aktenzeichen: 101 43 556.8
22 Anmeldetag: 6. 9. 2001
43 Offenlegungstag: 27. 3. 2003

DE 101 43 556 A 1

71 Anmelder:
DaimlerChrysler AG, 70567 Stuttgart, DE

72 Erfinder:
Dorner, Jürgen, Dipl.-Ing. (FH), 73101 Aichelberg,
DE; Heising, Thomas, Dipl.-Ing., 71540 Murrhardt,
DE; Kuhn, Anja, Dipl.-Ing., 70734 Fellbach, DE

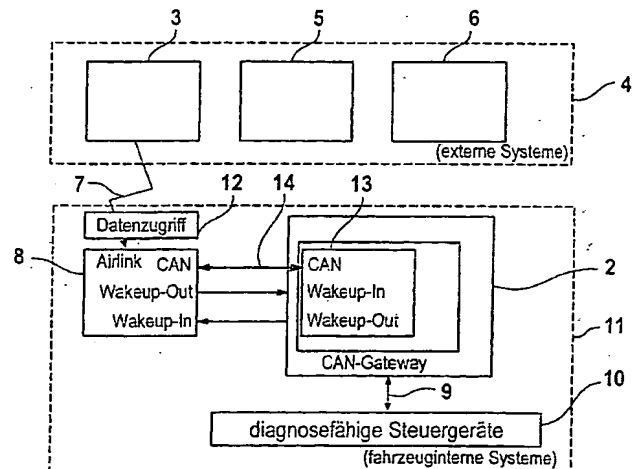
55 Für die Beurteilung der Patentfähigkeit in Betracht
zu ziehende Druckschriften:

DE 196 53 551 C1
DE 196 05 407 C2
DE 43 41 834 C1
DE 40 10 094 C2
DE 199 60 959 A1
DE 198 53 000 A1
DE 198 13 953 A1
DE 197 55 686 A1
DE 197 00 353 A1
DE 196 50 047 A1
DE 196 20 885 A1
DE 195 30 727 A1
DE 100 08 974 A1
DE 42 01 146 A1
DE 39 42 639 A1
DE 690 20 179 T2
DE 690 20 179 T2
DE 689 23 863 T2
EP 07 08 427 A2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

54 Fahrzeugmanagementsystem

57 Ein Fahrzeugmanagementsystem mit einem fahrzeug-
gebundenen Steuerrechner (2) und einer über eine draht-
lose Schnittstelle (7) mit dem Steuerrechner (2) verbunde-
nen zentralen Leitstelle (3), wobei der Steuerrechner eine
Kommunikationseinheit (8) zur Bereitstellung und Spei-
cherung der über die drahtlose Schnittstelle (7) zu über-
tragenden Daten und eine Datenbusschnittstelle (9) auf-
weist, um über einen Datenbus von im Fahrzeug angeor-
dneten Steuergeräten (10) verschiedene Sensordaten zu
erfassen. Erfindungsgemäß weist die Kommunika-
tionseinheit (8) ein Zugriffsberechtigungsprüfmittel (13) auf,
das bei einem Datenzugriff von der Leitstelle (3) die Zu-
griffsberechtigung des zugreifenden Teilnehmers prüft,
und dass das Zugriffsberechtigungsprüfmittel (13) eine
Berechtigungsmaske (18) vorsieht, die durch bitweise lo-
gische Verknüpfung mit einem von der Leitstelle (3) stam-
menden Datenzugriffs-Codewort (12) die Zugriffsberech-
tigung des Teilnehmers bestimmt.



DE 101 43 556 A 1

[0001] Die Erfindung betrifft ein Fahrzeugmanagementsystem mit einem fahrzeuggebundenen Steuerrechner und einer über eine drahtlose Schnittstelle mit dem Steuerrechner verbundene zentrale Leitstelle, wobei der Steuerrechner eine Kommunikationseinheit zur Bereitstellung und Speicherung der über die drahtlose Schnittstelle zu übertragenden Daten und eine Datenbusschnittstelle aufweist, um über den Datenbus von im Fahrzeug angeordneten Steuergeräten verschiedene Sensordaten zu erfassen.

[0002] Ein Fahrzeugmanagementsystem mit der Bezeichnung Fleetbord ist in den Verkehrsmitteln von DaimlerChrysler bereits im Einsatz. Dieses Fahrzeugmanagementsystem wird hauptsächlich bei schweren Lastkraftwagen eingesetzt. Aus den vom Fahrzeug an eine zentrale Leitstelle übertragenen Daten lassen sich bspw. der Fahrzeugstandort, der Zustand des Fahrzeugs, die Art der Waren, der Kühlzustand bei verderblichen Waren und diebstahlrelevante Daten ermitteln. Aufgrund der Daten können dann von der zentralen Leitstelle neue Aufträge oder Fahrtrouten, Diagnosedaten oder eine neue Software zur Reparatur von technischen Fehlern am Fahrzeug übermittelt werden.

[0003] Aus der EP 708 427 A2 ist ein Fahrzeugmanagementsystem bekannt, welches Fahrzeugdaten aufgrund von Sensoren im Fahrzeug erfasst und diese über eine Telematik-Schnittstelle an die zentrale Leitstelle übermittelt, um für den Fahrer oder den Logistik-Unternehmer verschiedene Dienst bereitzustellen. Im Fahrzeug ist ein Onboard-System vorhanden, welches die erforderlichen Daten der verschiedenen Sensoren empfängt und abspeichert. Die Sensordaten werden dabei über einen Datenbus und verschiedene Steuergeräte zu dem Onboard-System übermittelt. Insbesondere werden Fahrzeugdiagnosedaten zur Überwachung hinsichtlich technischer Defekte im Fahrzeug und Daten zur Fahrstrecke des Fahrzeugs im Onboard-System gespeichert und zu einer zentralen Leitstelle übermittelt. Von dort können dann die wichtigsten Fahrzeugfunktionen und die Fahrtroute des Fahrzeugs überwacht und über an das Fahrzeug zurückübertragene Daten angepasst werden.

[0004] Die DE 197 55 686 A1 zeigt ein Fahrzeugmanagementsystem mit mehreren in einem Fahrzeug angeordneten und vernetzten Steuereinheiten und einer vom Fahrzeug unabhängigen zentralen Leitstelle, die durch eine drahtlose Datenübertragungseinrichtung vom Fahrzeug übermittelte Daten sammelt, auswertet und neue Daten wieder ans Fahrzeug zurück überträgt. Im Fahrzeug ist ein Grundmodul vorhanden, das die von den einzelnen Steuereinheiten übermittelten Sensordaten speichert und auch eine Eingabe von Daten durch den Fahrer zulässt. Es ist auch vorgesehen, dass die Leitstelle Vorgaben für das Fahrzeugmanagement ändert und Nachrichten an den Fahrer überträgt.

[0005] Es ist Aufgabe der vorliegenden Erfindung, ein Fahrzeugmanagementsystem der eingangs genannten Art derart weiterzubilden, dass es im Zusammenhang mit Dienstbietern anderer Fahrzeughersteller flexibel einsetzbar ist. Dazu ist insbesondere eine verbesserte Zugriffsberechtigungsprüfung und die Bereitstellung eines Simulationsmodells für das Fahrzeug erforderlich.

[0006] Diese Aufgabe wird durch die Merkmale des unabhängigen Anspruchs 1 gelöst. Danach weist die Kommunikationseinheit ein Zugriffsberechtigungsmedium auf, das bei einem Datenzugriff von der Leitstelle die Zugriffsberechtigung des zugreifenden Teilnehmers prüft, und dass das Zugriffsberechtigungsprüfmittel eine Berechtigungsmaske vorsieht, die durch bitweise logische Verknüpfung mit einem von der Leitstelle stammenden Datenzugriffs-Codewort die Zugriffsberechtigung des Teilnehmers bestimmt.

[0007] Erfindungsgemäß prüft das Zugriffsberechtigungsprüfmittel jedes über die drahtlose Schnittstelle eingehende Datenzugriffs-Codewort auf dessen Zugriffsberechtigung. Bei einem Datenzugriff, beispielsweise bei der Übertragung eines Diagnose-Protokolls von der Leitstelle, hat das Datenzugriffs-Codewort ein vorgegebenes Format, beispielsweise 16 Byte. Mittels einer Berechtigungsmaske, die in der Datentlänge der Länge des Datenzugriffs-Codewort entspricht, ist eine Berechtigungsüberprüfung vorgesehen. Das von der Leitstelle eingehende Datenzugriffs-Codewort wird dazu bitweise mit der Berechtigungsmaske verglichen bzw. über eine logische "Oder-" oder "Und"-Verknüpfung bitweise verknüpft.

[0008] Neben der zur bitweisen logischen Verknüpfung vorgesehenen Berechtigungsmaske kann noch eine Bewertungsmaske vorgesehen sein, die bestimmt, welches Bit oder welchen Byte für die Beurteilung der Zugriffsberechtigung zu werten ist und welches Bit oder Byte im Zusammenhang mit der Zugriffsberechtigung nicht bewertet wird. Die Bewertungsmaske kann Bewertungs- und Don't-care-Stellen innerhalb der Maske festlegen.

[0009] Das Zugriffsberechtigungsprüfmittel kann durch bitweise Maskierung des Datenzugriffs-Codeworts zusätzlich bestimmen, auf welches der Steuergeräte von dem externen Teilnehmer über die Leitstelle zugegriffen werden kann. Außerdem kann über die bitweise Maskierung nur ein bestimmter Befehlssatz für den Steuerrechner oder die einzelnen Steuergeräte zugelassen sein.

[0010] Das Datenzugriffs-Codewort ist bevorzugt mit einem Datenformat vorgesehen, dass eine Absender- und Zielkennung und Datenfelder aufweist. Als Absenderkennung kann ein Name eines externen Teilnehmers, der auf Daten des Fahrzeugs zugreifen möchte, und als Zieladresse kann eine Steuergerätebezeichnung vorgesehen sein. In den Datenfeldern sind beispielsweise ein Steuerbefehl und die entsprechenden Parameter für diesen angeordnet. Die Berechtigungsmaske wird zumindest die Ziel- und Absenderadresse sowie den auszuführenden Steuerbefehl durch die Maskierung überprüfen. Bei einem positiven Prüfergebnis wird dem Empfänger erlaubt, mittels des Datenzugriffs-Codeworts auf das angegebene Steuergerät durchzugreifen und auf diesem Steuergerät den Befehl auszuführen. Dabei kann beispielsweise eine Datenabfrage bestimmter Sensordaten durch den Befehl ausgelöst werden, so dass die Daten wieder über die drahtlose Schnittstelle zur Leitstelle zurückübertragen werden.

[0011] Die Aufgabe wird auch durch die Merkmale des unabhängigen Anspruchs 4 gelöst. Danach weist die Kommunikationseinheit ein Zugriffsberechtigungsprüfmittel auf, das bei einem Datenzugriff von der Leitstelle die Zugriffsberechtigung des zugreifenden Teilnehmers prüft, dass eine Fahrzustandsprüfeinheit vorgesehen ist, die aufgrund von Sensordaten den Fahrzustand des Fahrzeugs ermittelt, und dass das Zugriffsberechtigungsprüfmittel ein Überschreiben von Daten in der Kommunikationseinheit nur zulässt, wenn die Fahrzustandsprüfeinheit einen dem Datenzugriff zugeordneten Fahrzustand des Fahrzeugs anzeigt.

[0012] Erfindungsgemäß wird dabei ein Datenzugriff mittels des Datenzugriffs-Codeworts zunächst auf eine Zugriffsberechtigung überprüft. Wird bei dem Datenzugriff beispielsweise eine Daten- oder Softwareänderung auf dem Steuerrechner oder einem Steuergerät des Fahrzeugs durchgeführt, muss sichergestellt sein, dass Datenschieben vorzugsweise nur bei einem stehenden Fahrzeug erlaubt ist. Eine Änderung der Software oder eine Veränderung von Parametern bei Steuergeräten während des Fahrzeugbetriebs kann Sicherheitsrisiken erzeugen. Deswegen ist eine Fahrzustandsprüfeinheit vorgesehen, die aufgrund von Sensor-

daten den Fahrzustand des Fahrzeug ermittelt.

[0013] Die Fahrzustandsprüfeinheit kann im Zusammenhang mit der Leitstelle vorgesehen sein, und beispielsweise von außerhalb des Fahrzeug die Fahrzeugpositionen feststellen. Dazu kann das Mobilfunknetz verwendet werden, woraus sich die Position des Fahrzeugs bestimmen lässt. Bevorzugt ist jedoch die Fahrzustandsprüfeinheit innerhalb des Fahrzeugs vorgesehen und die Fahrposition wird dann über ein GPS-System an Bord des Fahrzeugs ermittelt. Nur wenn das Fahrzeug steht und, insbesondere bei größeren Datenmengen auch durch ein Bremssystem gesichert ist, wird der Datenschreibvorgang ausgelöst. Lediglich das Lesen der Daten kann auch während der Fortbewegung des Fahrzeugs erlaubt werden, soweit die Zugriffsberechtigung durch das in Anspruch 1 beschriebene Zugriffsberechtigungsverfahren geprüft ist.

[0014] Durch die beiden Zugriffsberechtigungsverfahren besteht nun die Möglichkeit, das auch Anfragen externer Teilnehmer bearbeitet werden können, die nicht auf einer Software des Fahrzeugherstellers basieren. Dazu wird lediglich das Datenformat und die Absenderadresse vom Fahrzeughersteller festgelegt und der externe Teilnehmer kann dann auf bestimmte Informationen der Sensoren zugreifen, die vom Fahrzeughersteller für den externen Teilnehmer freigeschaltet sind. Beispielsweise kann ein Logistikunternehmer auf Sensordaten zurückgreifen, die beispielsweise die Temperatur in einem Anhänger eines Lastwagens angibt, der für einen gekühlten Lebensmitteltransport vorgesehen ist. Andererseits kann von einem Sicherheitsdienst zyklisch der Standort und der Zustand einer Alarmanlage innerhalb des Fahrzeugs, bzw. des Anhängers/Aufliegers, abgefragt werden.

[0015] Durch die Weiterbildung des Fahrzeugmanagementsystems und das spezielle Zugriffsberechtigungsverfahren können nun auch externe Teilnehmer, d. h. Kunden die bisher keine Möglichkeit für eine Datenabfrage aus den Steuergeräten des Netzwerks hatten, auf einzelne Funktionen innerhalb der Steuergeräte zugreifen. Durch die Berechtigungsmaske kann jedem externen Teilnehmer nur eine bestimmte Funktion, ein Steuerbefehl oder eine Zieladresse zugeordnet und bei Berechtigung ein bestimmter Zugriff darauf gestattet werden. Dadurch besteht sogar die Möglichkeit den Durchgriff auf sicherheitskritische Steuergerätefunktionen zuzulassen, wenn die Zugriffsberechtigung und die Fahrsituation dies erlauben.

[0016] Die Aufgabe wird erfindungsgemäß auch durch die Merkmale des Anspruchs 7 gelöst. Danach ist ein softwaregestütztes Simulationsmodell für das Fahrzeug vorgesehen, das über die Leitstelle ansprechbar ist. Aufgrund der vom Fahrzeug zur Leitstelle übertragenen Sensor- und Diagnosedaten kann die Funktionsfähigkeit des Fahrzeugs anhand des Simulationsmodells, bevorzugt in Echtzeit, überprüft werden. Dieses Simulationsmodell kann entweder im Steuerrechner oder bei der Leitstelle vorgesehen sein und aufgrund der Sensor- und Diagnosedaten des Fahrzeugs kann ein Fahrzustand oder ein Beladungszustand oder eine Fahrtroute eines Lastkraftwagens überprüft werden, bevor ein neuer Steuerbefehl an das Fahrzeug übermittelt wird.

[0017] Aufgrund des Simulationssystems besteht die Möglichkeit, für externe Teilnehmer mit Zugriffsberechtigung, gewisse Szenarios durchzuspielen, für die die Fahrtroute und der optimalen Fahrzustand des Fahrzeugs notwendig sind.

[0018] Es gibt nun verschiedene Möglichkeiten, die Lehre der vorliegenden Erfindung in vorteilhafter Weise auszugestalten und weiterzubilden. Dazu ist einerseits auf die untergeordneten Ansprüche und andererseits auf die nachfolgende Erläuterung einer Ausführungsform zu verweisen. In

der Zeichnung ist eine Ausführungsform der erfindungsgemäßen Vorrichtung zur Simulation dargestellt. Es zeigen jeweils in schematischer Darstellung,

[0019] Fig. 1 den Aufbau eines Fahrzeugmanagementsystems gemäß der vorliegenden Erfindung,

[0020] Fig. 2 ein Beispiel für eine Maskierung eines Datenzugriff-Codeworts nach einer Ausführungsform der vorliegenden Erfindung und

[0021] Fig. 3 eine Darstellung des Ablaufs bei einer Zugangsberechtigungsabfrage für ein Fahrzeugmanagementsystem gemäß der vorliegenden Erfindung.

[0022] Das Fahrzeugmanagementsystem 1 weist einen Steuerrechner 2 und eine zentrale Leitstelle 3 auf, die bezogen auf das Fahrzeug mit weiteren externen Systemen 4, beispielsweise dem Zentralrechner eines Logistikunternehmens 5 und dem Zentralrechner eines Sicherheitsdienstes 6 verbunden ist. Die Leitstelle 3 ist über eine drahtlose Schnittstelle 7 mit der Kommunikationseinheit 8 des Steuerrechners 2 verbunden. Der Steuerrechner 2 bildet zusammen mit der Kommunikationseinheit 8, der Datenbusschnittstelle 9 und den diagnosefähigen Steuergeräten 10 die fahrzeuginternen Systeme 11. Sobald von der Leitstelle 3 über die drahtlose Schnittstelle 7 ein Datenzugriff auf die Kommunikationseinheit 8 mittels eines Datenzugriffs-Codeworts 12 erfolgt, wird die drahtlose Schnittstelle 7 des Fahrzeugs automatisch durch ein sogenanntes Wakeup-Signal geweckt, wobei anschließend der Steuerrechner 2 durch ein weiteres Wakeup-Signal in einen Empfangszustand versetzt wird, so dass das Datenzugriffs-Codewort 12 im Steuerrechner durch ein Zugriffsberechtigungsprüfmittel 13 bearbeitet werden kann. Das Datenzugriffs-Codewort 12 kann dabei von der Kommunikationseinheit 8 der drahtlosen Schnittstelle 7 zum Steuerrechner 2 über einen Datenbus 14 übertragen werden.

[0023] Im Zugriffsberechtigungsprüfmittel 13 wird einerseits überprüft, ob das Datenzugriffs-Codewort 12, welches beispielsweise vom Zentralrechner des Logistikunternehmens 5 stammt und eine Positionsanfrage des Fahrzeugs darstellt, vorhanden ist. Dazu hat das Datenzugriffs-Codewort 12 ein vorbestimmtes Datenformat, in dem der Absendername, die Zieladresse, ein Steuerbefehl und weitere Daten vorgesehen sind. Aufgrund des bekannten Datenformats können bestimmte Bit- oder Byte-Positionen des Datenformats durch eine Maske diskriminiert werden, wobei dann bestimmte Codebereiche des Datenformats überprüft werden, während andere Bereiche des Datenformats unberücksichtigt (don't care) bleiben.

[0024] In Fig. 2 ist exemplarisch eines von einer Vielzahl von über die drahtlose Schnittstelle 7 nacheinander übertragenen Datenzugriffs-Codeworten 12 dargestellt. Das Datenzugriffs-Codewort 12 besteht dabei aus Adressierungsbereichen 15, Steuerbefehlsbereichen 16 und Datenbereichen 17. Das Datenformat der Datenbereiche 17 kann hierbei entsprechend der Anwendung oder eines Standards zu Datenübertragungsformaten variieren. Es muss lediglich vor der Datenübertragung ein Datenformat festgelegt sein, so dass die Kommunikationseinheit 8 die drahtlose Datenübertragung durchführen kann und das Zugriffsberechtigungsprüfmittel 13 mittels einer Berechtigungsmaske 18 die Adressierungsbereiche 15 mit der Absender- und Zieladresse diskriminieren kann. Die Berechtigungsmaske 18 weist eine Maskenbezeichnung 19 in Form eines Bytes auf, das eine spezielle von mehreren Masken bezeichnet. Ferner weist die Berechtigungsmaske 18 eine Diskriminierungsmatrix 20 auf, wobei für die nachfolgenden Steuer- und Datenbytes in der Berechtigungsmaske 18 jeweils ein Diskriminierungsbit vorhanden ist, wobei eine "1" angibt, dass das Steuer- bzw. Datenbyte geprüft werden muss und eine "0" angibt, dass

eine Prüfung für das Steuer- bzw. Datenbyte an der entsprechenden Stelle nicht erforderlich ist. Im Ausführungsbeispiel müssen die ersten vier Bytes im Adressierungsbereich 15 und das erste Byte im Steuerbefehlsbereich 16 auf die Berechtigung überprüft werden. Die übrigen Steuer- bzw. Datenbytes werden nicht überprüft und deswegen von der Berechtigungsmaske 18 ohne Änderung durchgelassen, was bei der logischen Verknüpfung, die im Ausführungsbeispiel in Form einer Hexadezimal-Addition durchgeführt wird, dazu führt, dass in der Berechtigungsmaske 18 an der entsprechenden Stelle ein "FF" eingetragen ist.

[0025] Durch die vorgesehene logische Verknüpfung, insbesondere eine ODER-Verknüpfung, ergibt sich immer dann ein berechtigtes Datenzugriffs-Codewort 21, wenn es nach der Prüfung auf Zugriffsberechtigung mit dem ursprünglichen Datenzugriffs-Codewort 12 übereinstimmt. Dies ist immer dann der Fall, wenn an der entsprechenden Stelle der Berechtigungsmaske 18 ein "FF" an der Byteposition eingetragen ist oder wenn wie in dem ersten Byte des Adressierungsbereichs 15 sowohl in der Berechtigungsmaske 18 als auch im Datenzugriffs-Codewort 12 die gleiche Bitfolge eingetragen ist. Dies ist im Beispiel die "18". Auf diese Weise kann durch die Berechtigungsmaske 18 lediglich eine Gruppe von Steuerbefehlsbereichen 16 zugelassen werden, wobei beispielsweise die Steuerbefehle, deren Steuerbefehlsbereich 16 mit dem Wert 1 A beginnt, lediglich das Auslesen von Daten und das Speichern von Daten bei stehendem Fahrzeug zulässt. Die unterschiedlichen Steuerbefehle sind dann in den folgenden Bytes des Steuerbefehlsbereichs 16 differenziert. Der Fahrzeughersteller ist daher in der Lage bestimmte externe Datenübertragungen von fremden Diensteanbietern über die Berechtigungsmaske 18 manipulierbar zuzulassen und Anfragen anderer Nutzer gegen unerwünschtes Datenlesen zu sperren.

[0026] Die Berechtigungsmaske 18 ist dabei im Wesentlichen bitmaskiert, dass heißt, obwohl in Fig. 2 byteweise dargestellt, kann die Berechtigungsmaske 18 in Bezug auf jedes Bit veränderbar sein. Die Berechtigungsmaske kann zusätzlich verschlüsselt werden, um einen externen Zugriff zu verhindern. Gerade diese erhöhte Datensicherheit und die Zugriffsberechtigungsprüfung ermöglicht es, dass vom Kunden auch ein Zugriff auf bestimmte Steuerungsfunktionen innerhalb des Fahrzeugs vorgenommen werden können. Dazu kann beispielsweise die Kühltemperatur in einem Auflieger eines Lastkraftwagens von einem externen System aus gesteuert werden oder es kann auch eine Alarmanlage durch eine Übertragung eines Datenzugriffs-Codeworts 12 über die drahtlose Schnittstelle 7 wieder abgeschaltet werden.

[0027] In Fig. 3 ist der zeitliche Ablauf einer Zugriffsberechtigungsprüfung dargestellt. Beim Starten eines Fahrzeugs wird zunächst geprüft, ob die Kommunikationseinheit 8 und das Zugriffsberechtigungsprüfmittel 13 des Steuerrechners 2 jeweils vollständig initialisiert sind. Ferner wird überprüft ob am Steuerrechner ein Tester, beispielsweise zur Erstellung einer Werkstattdiagnose, angeschlossen ist. Nach dem Selbsttest der Kommunikationseinheit 8 auf Kommunikationsfähigkeit und Prüfung der einzelnen Berechtigungsmasken im Zugriffsberechtigungsmittel 13 ist die Initialisierungsphase abgeschlossen und in der Folge werden eingehende Datenzugriffs-Codeworte 12 von der Kommunikationseinheit 8 empfangen und dem Zugriffsberechtigungsprüfmittel zur Diskriminierung durch die Berechtigungsmaske 18 übergeben. Als Ergebnis der verschiedenen eingehenden Datenzugriffs-Codeworte 12 (ID1...IDn) werden lediglich berechtigte Datenzugriffs-Codeworte 21 zur Weiterbearbeitung an den Steuerrechner 2 und zur dortigen Speicherung durchgelassen.

[0028] Durch das beschriebene Verfahren können externe Kunden auf Fahrzeuge bzw. Fahrzeugflotten eines Fahrzeugherstellers per Telematik schnell und flexibel zugreifen, wenn diese zuvor durch eine Zugriffsberechtigung freigeschaltet sind. Die Kommunikationseinheit 8 ist als Telematikplattform ausgebildet, die auch für andere Telematikdienste des Fahrzeugherstellers verwendet wird.

[0029] Das Zugriffsberechtigungsprüfmittel 13 sammelt fahrzeuginterne Daten, beispielsweise Zündung aus, Bremsen betätigt, und speichert diese Daten nach Abschluss einer Fahrt, wenn beim Zugriffsberechtigungsprüfmittel 13 ein bestimmter Befehl vorliegt. Diese Tourdaten eines Fahrzeugs können dann beispielsweise über einen externen Dienst eines Logistik-Unternehmens 5 über dessen Zentralrechner abgerufen werden, soweit dieser Dienst freigeschaltet ist. Die Tourdaten können im einfachsten Fall als SMS-Botschaften oder als Internetseite an den Zentralrechner 5 über die drahtlose Schnittstelle 7 übertragen werden. Das auf dem beschriebenen Fahrzeugmanagementsystem 1 durchführbare Verfahren kann an zukünftige Bedürfnisse der Kunden angepasst werden, indem die Zugriffsberechtigungsmasken flexibel parametrisierbar sind. Zur erhöhten Sicherheit können auch mehrere Berechtigungsmasken 18 mit dem eingehenden Datenzugriffs-Codewort 12 verglichen werden. Es kann dabei ein Vergleich mittels einer Positivliste und dann ein Vergleich mittels einer Negativliste durchgeführt werden, wobei aus den nicht geprüften Bytes oder Bitstellen ganz spezielle Steuerbefehle oder Zieladressen gesperrt werden können. Auch wenn eine Zugriffsberechtigung durch das Zugriffsberechtigungsprüfmittel 13 nicht vergeben wird, können bestimmte Daten an den Kunden zurückübertragen werden. Beispielsweise können dann Adressen für die Erlangung einer Zugriffsberechtigung angegeben werden oder eine Fehlermeldung rückübertragbar sein.

[0030] Der externe Zentralrechner 5 sendet dann eine erste Anfrage zur Kommunikationseinheit 8 des Fahrzeugs. Nach erfolgreichem Empfang der Anfrage wird eine Diagnosebotschaft nach der Zugriffsberechtigungsprüfung an den Steuerrechner 2 über einen Telematik-CAN-Datenbus übermittelt. Die Anfrage wird dann im Steuerrechner ausgewertet und der Diagnoseeinsatz kann durchgeführt werden. Außerdem kann ein Update der Software innerhalb des Fahrzeugs und die Softwarezustandsinformation an die Leitstelle 3 übertragen werden, um den Softwarezustand innerhalb des Fahrzeug zu dokumentieren.

[0031] Bei einer anderen Ausführungsform kann aus den vom Zugriffsberechtigungsprüfmittel 13 abgefragten Sensordaten des Fahrzeugs ein Simulationsmodell innerhalb des Steuerrechners 2 oder bei der Leitstelle 3 abgelegt werden, dass ein spezialisiertes Beschreibungsmodell des Fahrzeugs vorsieht. Die einzelnen Sensordaten können mittels Symbolen dargestellt werden und aufgrund der Sensordaten kann ein Fahrzustand, eine Fahrtroute, die momentane Fahrsituation oder die noch zu erwartende Fahrzeit berechnet werden. Das Simulationsmodell kann für den Kunden verbesserte Informationen über das Fahrzeug bereitstellen, soweit eine Zugriffsberechtigung dafür vergeben ist. Außerdem kann aufgrund des Simulationsmodells auch entschieden werden, ob ein Datenzugriff auf das Fahrzeug in der momentanen Fahrsituation möglich ist. Beispielsweise kann das Simulationsmodell die Situation der Ladung und des Fahrzeugs berechnen und daher Informationen über einen sicheren Standort des Fahrzeugs ermitteln. Wird aufgrund des Simulationsmodells ein sicherer Fahrzeugstandort erkannt, so kann ein Datenschieben auf das Fahrzeug zugelassen werden. Beispielsweise kann dann neue Software auf das Fahrzeug übertragen, dass heißt, geflasht werden, oder

Fehlercodes, Messwerte, Parameter und andere Daten können auf den Steuerrechner des Fahrzeugs übertragen werden.

[0032] Zu den externen Systemen zählen neben Kundensystemen auch bestimmte Server, Parametrier- oder Flashstationen und Diagnosetester.

Patentansprüche

1. Fahrzeugmanagementsystem mit einem fahrzeuggebundenen Steuerrechner (2) und einer über eine drahtlose Schnittstelle (7) mit dem Steuerrechner (2) verbundene zentralen Leitstelle (3), wobei der Steuerrechner (2) eine Kommunikationseinheit (8) zur Bereitstellung und Speicherung der über die drahtlose Schnittstelle (7) zu übertragenden Daten und eine Datenbusschnittstelle (9) aufweist, um über einen Datenbus von im Fahrzeug angeordneten Steuergeräten (10) verschiedene Sensordaten zu erfassen, **dadurch gekennzeichnet**, dass die Kommunikationseinheit (8) ein Zugriffsberechtigungsprüfmittel (13) aufweist, das bei einem Datenzugriff von der Leitstelle (3) die Zugriffsberechtigung des zugreifenden Teilnehmers (3, 5, 6) prüft, und dass das Zugriffsberechtigungsprüfmittel (13) eine Berechtigungsmaske (18) vorsieht, die durch bitweise logische Verknüpfung mit einem von der Leitstelle (3) stammenden Datenzugriffs-Codewort (12) die Zugriffsberechtigung des Teilnehmers (3, 5, 6) bestimmt.
2. Fahrzeugmanagementsystem nach Anspruch 1, dadurch gekennzeichnet, dass das Zugriffsberechtigungsprüfmittel (13) durch bitweise Maskierung zusätzlich bestimmt, auf welches der Steuergeräte (10) das Datenzugriffs-Codewort (12) zugreifen kann.
3. Fahrzeugmanagementsystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass das Zugriffsberechtigungsprüfmittel (13) durch bitweise Maskierung zusätzlich bestimmt, welcher Befehl bei welchem Steuergerät (10) zulässig ist.
4. Fahrzeugmanagementsystem mit einem fahrzeuggebundenen Steuerrechner (2) und einer über eine drahtlose Schnittstelle (7) mit dem Steuerrechner (2) verbundene zentralen Leitstelle (3), wobei der Steuerrechner (2) eine Kommunikationseinheit (8) zur Bereitstellung und Speicherung der über die drahtlose Schnittstelle (7) zu übertragenden Daten und eine Datenbusschnittstelle (9) aufweist, um über einen Datenbus von im Fahrzeug angeordneten Steuergeräten (10) verschiedene Sensordaten zu erfassen, dadurch gekennzeichnet, dass der Steuerrechner (2) ein Zugriffsberechtigungsprüfmittel (13) aufweist, dass bei einem Datenzugriff von der Leitstelle (3) die Zugriffsberechtigung des zugreifenden Teilnehmers prüft, dass eine Fahrzustandsprüfeinheit vorgesehen ist, die aufgrund von Sensordaten den Fahrzustand des Fahrzeugs ermittelt, und dass das Zugriffsberechtigungsprüfmittel (13) ein Überschreiben von Daten in der Kommunikationseinheit (8) nur zulässt, wenn die Fahrzustandsprüfeinheit einen dem Datenzugriff (12) zugeordneten Fahrzustand des Fahrzeugs anzeigt.
5. Fahrzeugmanagementsystem nach Anspruch 4, dadurch gekennzeichnet, dass die Fahrzustandsprüfeinheit als Bestandteil des Steuerrechners (2) oder eines Steuergerätes (10) vorgesehen ist.
6. Fahrzeugmanagementsystem nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass die Fahrzustandsprüfeinheit ein Schreiben von Daten im Fahrzeug nur bei dessen Stillstand zulässt.

7. Fahrzeugmanagementsystem mit einem fahrzeuggebundenen Steuerrechner (2) und einer über eine drahtlose Schnittstelle (7) mit dem Steuerrechner (2) verbundene zentralen Leitstelle (3), wobei der Steuerrechner (2) eine Kommunikationseinheit (8) zur Bereitstellung und Speicherung der über die drahtlose Schnittstelle (7) zu übertragenden Daten und eine Datenbusschnittstelle (9) aufweist, um über einen Datenbus von im Fahrzeug angeordneten Steuergeräten (10) verschiedene Sensordaten zu erfassen, dadurch gekennzeichnet, dass ein softwaregestütztes Simulationsmodell für das Fahrzeug mit der Leitstelle (3) in Verbindung steht und aufgrund der vom Fahrzeug zur Leitstelle (3) übertragenen Sensor- und Diagnosedaten die Funktionsfähigkeit des Fahrzeugs anhand des Simulationsmodells überprüfbar ist.

8. Fahrzeugmanagementsystem nach Anspruch 7, dadurch gekennzeichnet, dass die Simulation des Fahrzeugs mit den IST-Sensordaten des Fahrzeugs durchführbar ist.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

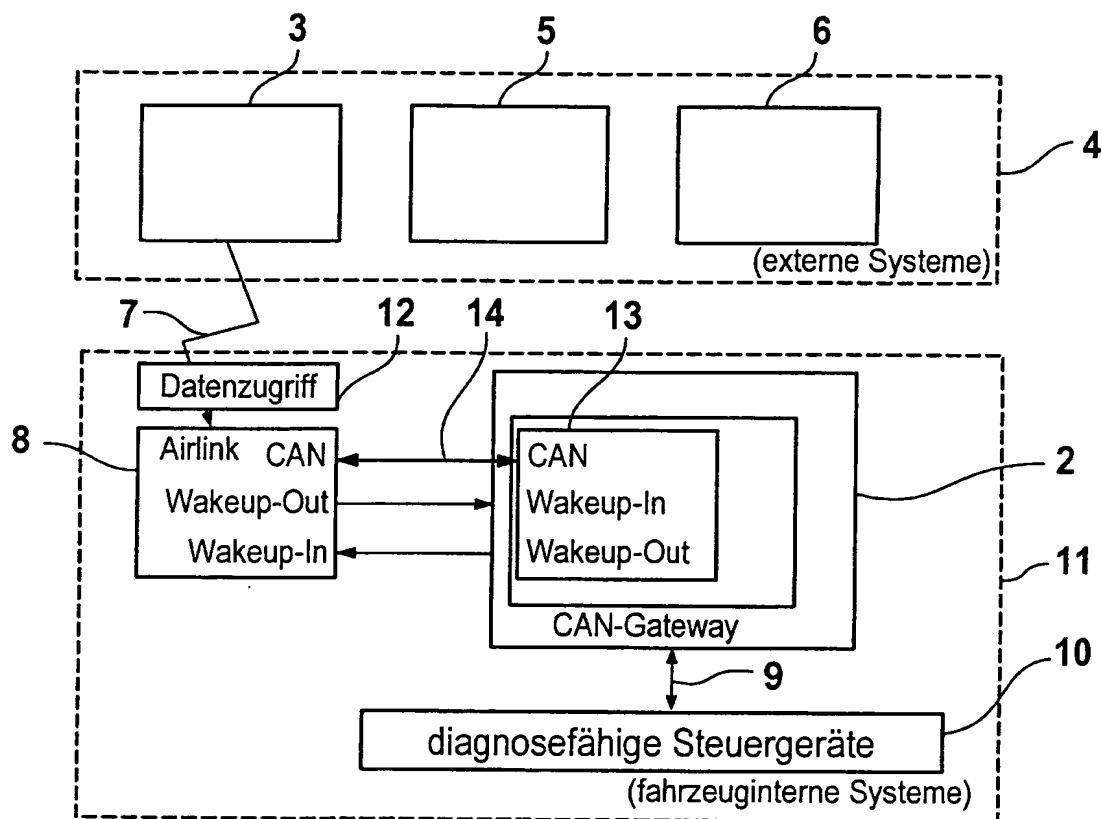


Fig. 1

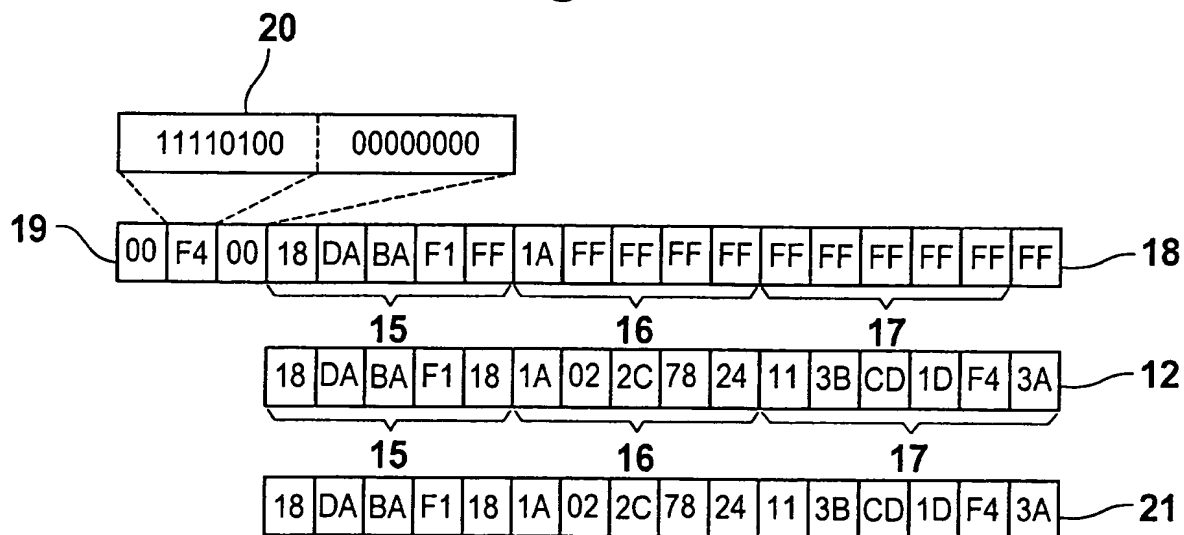


Fig. 2

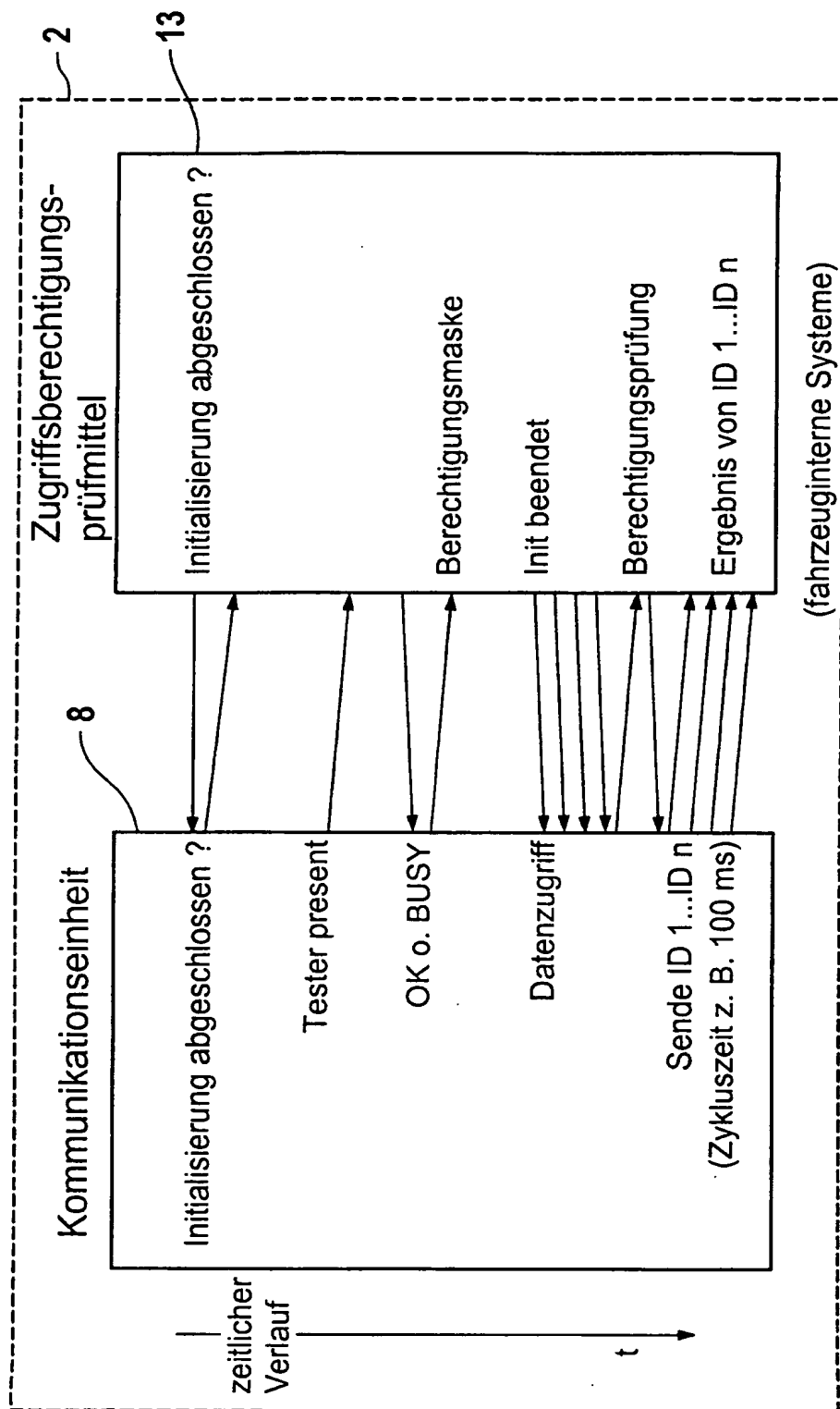


Fig. 3